UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,132	11/14/2001	Charles F. Hawkins	COM001	6186

32435 7590 09/30/2005

SETO PATENTS
406 RIVERLAND DR.
SALEM, VA 24153

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/993,132	HAWKINS ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on November 14, 2001. Claims 1-61 were originally received for consideration. No preliminary amendments for the claims were received. Claims 1-61 are currently being considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-4, 30-31, and 34-37 are rejected under 35 U.S.C. 102(b) as being anticipated by Bisbee et al. (U.S. Patent No. 5,748,738).

Regarding claim 1, Bisbee discloses:

A method for creating a unique authoritative electronic record, comprising the steps of:

receiving an electronic record into a repository, wherein the repository is contained on an electronic device that stores and executes software (column 6 lines 46-59), wherein the authentication center stores received documents;

generating a receipt, wherein the receipt includes information relating to the electronic record (column 5 line 56 – column 6 line 13), wherein the integrity block is appended to the document and comprises digital signatures, time stamps, and other information used to eliminate the possibility of unauthorized tampering or alteration;

generating identifying information that includes a provable representation of the receipt (column 3 lines 13-20), wherein the identifying information is interpreted as a certificate which contains the digital signatures;

prepending the receipt to a beginning of the record (column 5 line 56 – column 6 line 13), wherein it is interpreted that the integrity block is appended to the beginning of the document in order to properly identify the authenticity of the document;

appending the identifying information to an ending of the record (Figure 9, column 10 lines 50-65); and,

storing the record with the prepended receipt and the appended identifying information as the unique authoritative record in the repository (column 5 line 56 – column 6 line 13, column 6 lines 43-59), wherein the document is stored with the integrity block which eliminates the possibility of unauthorized alteration or tampering.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Bisbee discloses:

The method of claim 1, wherein the step of receiving a record further comprises the step of attaching a time-stamp to the electronic record, wherein the time-stamp includes a time and a date when the electronic record was received in the repository

and identification information (column 5 line 64 – column 6 line 13).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Bisbee discloses:

The method of claim 1, wherein the receipt comprises a digital signature made with a private key of the repository (column 5 line 64 – column 6 line 13).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Bisbee discloses:

The method of claim 1, wherein the repository creates a copy of the authoritative record by copying the record and all information appended to the ending of the record (column 9 lines 27-41), wherein a request for a copy of the document is sent to a transfer agent to be signed, and wherein the integrity block (header) is not transmitted.

Regarding claim 30, Bisbee discloses:

A computer readable medium for storing a program that allows a user to receive, and digitally sign a copy of an electronic record that is stored in a remote location, wherein the program provides for the user to:

receive a proper subset of the electronic record, wherein the proper subset of the electronic record allows the user to view, store and print the record, and when the user is ready, to (column 9 lines 50-57, column 10 lines 50-64), wherein the transfer agent (remote location) digitally signs the document ;

sign the electronic record, wherein the program requests and receives at least a complement of the proper subset of the electronic record, and the user then uses the proper subset, the complement of the subset, and a private key to digitally sign the record (column 10 lines 23-49), wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature.

Clam 31 is rejected as applied above in rejecting claim 31. Furthermore, Bisbee discloses:

The computer readable medium of claim 30, wherein the program provides for transmission of the digital signature to the remote location (Figure 7, column 10 line 50 – column 11 line 12), wherein the signed document is transmitted to the authentication center (secure environment) for authentication and storage (column 10 lines 4-7).

Regarding claim 34, Bisbee discloses:

An apparatus for creating and storing a unique authoritative record, comprising:

at least one server, connected to a network, that stores and executes software for receiving a record in a secure environment wherein the secure environment is created by the server and the software (column 6 lines 46-59), wherein the authentication center stores documents;

wherein the software provides for:

generating a receipt, wherein the receipt includes information relating to the record (column 5 line 56 – column 6 line 13), wherein the integrity block is appended to the document and comprises digital signatures, time stamps, and other information used to eliminate the possibility of unauthorized tampering or alteration;

generating identifying information that includes a provable representation of the receipt (column 3 lines 13-20), wherein the second information is interpreted as the message digest and/or signature;

prepending the receipt to a beginning of the record (column 5 line 56 – column 6 line 13, column 6 lines 43-59), wherein the document is stored with the integrity block which eliminates the possibility of unauthorized alteration or tampering;

appending the identifying information to an ending of the record (Figure 9, column 10 lines 50-65), wherein a certificate containing the signatures is added to the electronic document; and,

storing the record with prepended receipt and appended information as the unique authoritative record in the secure environment (column 5 line 56 – column 6 line 13, column 6 lines 43-59), wherein the document is stored with the integrity block which eliminates the possibility of unauthorized alteration or tampering.

Claim 35 is rejected as applied above in rejecting claim 34. Furthermore, Bisbee discloses:

The apparatus of claim 34, wherein the record is time-stamped, with a time and date the record was received and with identification information, immediately after the

record is received in the secure environment (column 5 line 64 – column 6 line 13).

Claim 36 is rejected as applied above in rejecting claim 34. Furthermore, Bisbee discloses:

The apparatus of claim 34, wherein the receipt comprises a digital signature made with a private key of the secure environment (column 5 line 64 – column 6 line 13).

Claim 37 is rejected as applied above in rejecting claim 34. Furthermore, Bisbee discloses:

The apparatus of claim 34, wherein the secure environment creates a copy of the authoritative record by copying the record and all information appended to the ending of the record (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed, and wherein the integrity block (header) is not transmitted but a message digest is transmitted.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 5-29, 32-33, and 38-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bisbee et al. (U.S. Patent No. 5,748,738) in view of Vantsone (U.S. Patent No. 6,212,281).

Regarding claim 5, Bisbee discloses:

A method for obtaining a digital signature on an authoritative record stored in a secure environment, comprising the steps of:

receiving a request to sign the authoritative record (column 9 lines 27-41), wherein in response to a request for the document, a copy of the document is sent to the transfer agent for signing;

computing a complement of the proper subset (column 9 lines 27-41), wherein a request for the copy of the document is sent to a transfer agent (remote location) to be signed, and wherein the integrity block (header) is not sent;

computing a message digest, at the remote location, using the partial message digest and the complement of the subset (column 10 lines 23-49), wherein the partial message digest is decrypted and the encrypted key is retrieved from the hash ; and,

creating a digital signature with the use of the message digest and a private key (column 10 lines 33-43), wherein the digest is encrypted using the remote location's secret (private) key and produces the signature.

Bisbee does not explicitly disclose generating, at the secure location and sending, to a remote location, the partial message digest of the beginning information at the secure

environment, along with the document and ending information (complement). Vanstone discloses generating a hash (message digest) of a part (partial) of a document, which can be the header, and sending the partial digest to a recipient who can sign the document (column 3 line 65 – column 4 line 26). Bisbee and Vanstone are analogous arts because both are concerned with digitally signing documents, and both use a private key and a digest to calculate the signature. Vanstone states that the "it is usual for the message to include some redundancy" (column 1 lines 47-54) and further states that the accuracy of the message is insured by the hash (digest) (column 2 lines 45-55). Therefore, it would have been obvious to generate the message digest at the secure environment and then transmitting it to the remote location to verify the integrity of the message and provide redundancy in the message.

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Bisbee discloses:

The method of claim 5, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record (column 3 line 65 – column 4 line 26), wherein the integrity block (header) would have been an obvious choice for being hashed because it contains the digital signature, and verifies the authenticity of the document.

Claim 7 is rejected as applied above in rejecting claim 5. Furthermore, Bisbee discloses:

The method of claim 5, wherein the complement of the proper subset of the authoritative record comprises an electronic record and ending information that is appended an end of the record (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed, and wherein the integrity block (header) is not transmitted but a message digest is transmitted.

Claim 8 is rejected as applied above in rejecting claim 5. Furthermore, Bisbee discloses:

The method of claim 5, wherein the step of sending further comprises the steps of sending the partial message digest and the complement of the proper subset of the authoritative record to the remote location (column 9 lines 27-41), wherein a request for the copy of the document is sent to a transfer agent (remote location) to be signed, and wherein the integrity block (header) is not sent.

Claim 9 is rejected as applied above in rejecting claim 5. Furthermore, Bisbee discloses:

The method of claim 5, wherein software associated with the secure environment is used at the remote location (column 7 lines 23-34), wherein both the secure environment (authentication center) and the remote location (transfer agent) are capable of producing digital signatures.

Claim 10 is rejected as applied above in rejecting claim 5. Furthermore, Bisbee discloses:

The method of claim 5, further comprising the step of:

transmitting the digital signature to the secure environment (Figure 7, column 10 line 50 – column 11 line 12), wherein the signed document is transmitted to the authentication center (secure environment) for authentication and storage.

Regarding claim 11, Bisbee discloses:

A method for creating a unique authoritative record, obtaining and validating a digital signature on the authoritative record, and upon successful validation creating a unique revised authoritative record, comprising the steps of:

receiving a record in a secure environment, wherein the secure environment is connected to a network and comprises at least one server that stores and executes software (column 6 lines 46-59), wherein the authentication center stores documents;

generating a receipt, wherein the receipt includes information relating to the record (column 5 line 56 – column 6 line 13), wherein the integrity block is appended to the document and comprises digital signatures, time stamps, and other information used to eliminate the possibility of unauthorized tampering or alteration;

generating identifying information that includes a provable representation of the receipt (column 3 lines 13-20), wherein the second information is interpreted as a certificate containing signatures;

prepending the receipt to a beginning of the record (column 5 line 56 – column 6 line 13), wherein the integrity block is appended to the document and comprises digital signatures, time stamps, and other information used to eliminate the possibility of unauthorized tampering or alteration;

appending the identifying information to an ending of the record (Figure 9, column 10 lines 50-65), wherein a certificate containing the signatures is added to the electronic document;

storing the record with prepended receipt and appended information as the unique authoritative record (column 5 line 56 – column 6 line 13, column 6 lines 43-59), wherein the document is stored with the integrity block which eliminates the possibility of unauthorized alteration or tampering;

receiving a request to sign the authoritative record (column 9 lines 27-41), wherein in response to a request for the document, a copy of the document is sent to the transfer agent for signing;

computing a message digest, at the remote location, using the partial message digest and the complement of the subset (column 10 lines 23-49), wherein the partial message digest is decrypted and the encrypted key is retrieved from the hash;

creating a digital signature with the use of the message digest and a private key (column 10 lines 33-43), wherein the digest is encrypted using the remote location's secret (private) key and produces the signature;

transmitting the digital signature to the secure environment (Figure 7, column 10 line 50 – column 11 line 12), wherein the signed document is transmitted to the

authentication center (secure environment) for authentication and storage (column 10 lines 4-7);

validating the digital signature in the secure environment, and upon affirmative validation (column 10 line 65 – column 11 line 12);

revising the authoritative record with the digital signature to create a revised authoritative record (column 10 line 65 – column 11 line 23), wherein after the signature is validated, the document is confirmed and guaranteed and stored (column 10 lines 1-7), and furthermore, a certificate with all the signature of the Certification Authorities of the signers is appended to the end of the document.

Bisbee does not explicitly disclose generating, at the secure location and sending, to a remote location, the partial message digest of the beginning information at the secure environment, along with the document and ending information (complement). Vanstone discloses generating a hash (message digest) of a part (partial) of a document, which can be the header, and sending the partial digest to a recipient who can sign the document (column 3 line 65 – column 4 line 26). Bisbee and Vanstone are analogous arts because both are concerned with digitally signing documents, and both use a private key and a digest to calculate the signature. Vanstone states that the "it is usual for the message to include some redundancy" (column 1 lines 47-54) and further states that the accuracy of the message is insured by the hash (digest) (column 2 lines 45-55). Therefore, it would have been obvious to generate the message digest at the secure

environment and then transmitting it to the remote location to verify the integrity of the message and provide redundancy in the message.

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Bisbee discloses:

The method of claim 11, wherein the step of receiving a record further comprises time-stamping the record, wherein a time-stamp comprising a time and date the record was received and identification information is attached to the record and the time-stamped record is used as the record in subsequent steps (column 5 line 64 – column 6 line 13).

Claim 13 is rejected as applied above in rejecting claim 11. Furthermore, Bisbee discloses:

The method of claim 11, wherein the receipt is a digital signature that is made with a private key of the secure environment (column 5 line 64 – column 6 line 13).

Claim 14 is rejected as applied above in rejecting claim 11. Furthermore, Bisbee discloses:

The method of claim 11, wherein the proper subset of the authoritative record comprises information at a beginning of the authoritative record (column 3 line 65 – column 4 line 26), wherein the integrity block (header) would have been an obvious choice for being hashed because it contains the digital signature, and verifies the

authenticity of the document.

Claim 15 is rejected as applied above in rejecting claim 11. Furthermore, Bisbee discloses:

The method of claim 11, wherein the complement of the proper subset of the authoritative record comprises the record and ending information that is appended an end of the record (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed, and wherein the integrity block (header) is not transmitted but a message digest is transmitted.

Claim 16 is rejected as applied above in rejecting claim 11. Furthermore, Bisbee discloses:

The method of claim 11, wherein the step of sending further comprises the steps of sending the partial message digest and the complement of the proper subset of the authoritative record to the remote location in two separate transmissions (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed, and wherein the integrity block (header) is not transmitted but a message digest is transmitted.

Claim 17 is rejected as applied above in rejecting claim 11. Furthermore, Bisbee discloses:

The method of claim 11, wherein software associated with the secure environment is used at the remote location (column 7 lines 23-34), wherein both the secure environment (authentication center) and the remote location (transfer agent) are capable of producing digital signatures.

Regarding claim 18, Bisbee discloses:

A method for creating and validating at least one digital signature for an electronic authoritative record maintained in a secure environment, wherein control is maintained in the secure environment by software and at least one server, and a copy of the electronic authoritative record can be electronically transmitted to a remote location without losing any of the electronic authoritative record's integrity, the method comprising the steps of:

receiving an electronic record in the secure environment (column 6 lines 46-59), wherein the authentication center stores documents;

generating at least some first information comprising a receipt of the electronic record by the secure environment (column 5 line 56 – column 6 line 13), wherein the integrity block is appended to the document and comprises digital signatures, time stamps, and other information used to eliminate the possibility of unauthorized tampering or alteration;

defining a beginning information as all information prepended to a beginning of the record and comprising the first information (column 5 line 56 – column 6 line 13), wherein the integrity block is appended to the document and comprises digital

signatures, time stamps, and other information used to eliminate the possibility of unauthorized tampering or alteration;

generating at least some second information comprising a provable representation of the first information, wherein the provable representation is mathematically related to the first information (column 3 lines 13-20), wherein the second information is interpreted as the message digest and/or signature;

defining an ending information as all information appended to an end of the record and comprising the second information (Figure 9, column 10 lines 50-65), wherein a certificate containing the signatures is added to the electronic document;

creating an authoritative record comprising the beginning information, the electronic record, and the ending information, wherein the beginning information is prepended to the beginning of the electronic record and the ending information is appended to the end of the electronic record (column 5 line 56 – column 6 line 13, column 6 lines 43-59), wherein the document is stored with the integrity block which eliminates the possibility of unauthorized alteration or tampering;

storing the authoritative record in the secure environment (column 5 line 56 – column 6 line 13, column 6 lines 43-59), wherein the document is stored with the integrity block which eliminates the possibility of unauthorized alteration or tampering;

making a perceivable copy of the authoritative record by copying only the electronic record and the ending information (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed, and

wherein the integrity block (header) is not transmitted but a message digest is transmitted;

transmitting the perceivable copy of the authoritative record to a remote location (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed;

receiving the perceivable copy at the remote location, and if desired digitally signing the authoritative record (column 9 lines 50-57, column 10 lines 50-64), wherein the transfer agent (remote location) digitally signs the document;

completing a message digest of the authoritative record at the remote location with the use of the partial message digest and the perceivable copy (column 10 lines 23-49), wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature;

creating a digital signature using the message digest at the remote location and a private key to produce a digital signature of the authoritative record (column 10 lines 33-43), wherein the digest is encrypted using the remote location's secret (private) key and produces the signature;

transmitting the digital signature from the remote location to the secure environment (Figure 7, column 10 line 50 – column 11 line 12), wherein the signed document is transmitted to the authentication center (secure environment) for authentication and storage (column 10 lines 4-7);

receiving the digital signature in the secure environment (Figure 7, column 10 line 50 – column 11 line 12), wherein the signed document is transmitted to the authentication center (secure environment) for authentication;

validating the digital signature in the secure environment with the use of the digital signature, a corresponding public key of the private key, and a separately computed message digest of the authoritative record in the secure environment, and upon affirmative validation of the digital signature (column 10 line 65 – column 11 line 12);

generating a revised authoritative record by prepending digital signature information comprising the digital signature to a beginning of the authoritative record, wherein the digital signature information is thereby included in the beginning information, appending signature information comprising of a provable representation of the digital signature information to an end of the authoritative record, wherein the ending information thereby includes the signature information (column 10 line 65 – column 11 line 23), wherein after the signature is validated, the document is confirmed and guaranteed and stored (column 10 lines 1-7), and furthermore, a certificate with all the signature of the Certification Authorities of the signers is appended to the end of the document;

storing the revised authoritative record in the secure environment (column 10 lines 1-7).

Bisbee does not explicitly disclose generating, at the secure location and transmitting, to a remote location, the partial message digest of the beginning information at the secure environment. Vanstone discloses generating a hash (message digest) of a part (partial) of a document and sending the partial digest to a recipient who can sign the document (column 3 line 65 – column 4 line 26). Bisbee and Vanstone are analogous arts because both are concerned with digitally signing documents, and both use a private key and a digest to calculate the signature. Vanstone states that the "it is usual for the message to include some redundancy" (column 1 lines 47-54) and further states that the accuracy of the message is insured by the hash (digest) (column 2 lines 45-55). Therefore, it would have been obvious to generate the message digest at the secure environment and then transmitting it to the remote location to verify the integrity of the message and provide redundancy in the message.

Claim 19 is rejected as applied above in rejecting claim 18. Furthermore, Bisbee discloses:

The method of claim 18, wherein the step of generating a revised authoritative record, further comprises:

prepending a signature receipt to the beginning information so that the signature receipt becomes part of the beginning information, wherein the signature receipt comprises a unique representation of the revised authoritative record (column 10 line 65 – column 11 line 23), wherein after the signature is validated, the document is confirmed

and guaranteed and stored (column 10 lines 1-7), and furthermore, a certificate with all the signature of the Certification Authorities of the signers is appended to the end of the document; and,

appending identifying information to the ending information so that the identifying information becomes part of the ending information, wherein the identifying information comprises a provable representation of the signature receipt (Figure 9, column 10 lines 50-65), wherein a certificate containing the signatures is added to the electronic document.

Claim 20 is rejected as applied above in rejecting claim 18. Furthermore, Bisbee discloses:

The method of claim 18, wherein software associated with the secure environment is stored and used at the remote location (column 7 lines 23-34), wherein both the secure environment (authentication center) and the remote location (transfer agent) are capable of producing digital signatures.

Claim 21 is rejected as applied above in rejecting claim 18. Furthermore, Bisbee discloses:

The method of claim 18, wherein the perceivable copy and the partial message digest are transmitted to the remote location in a same transmission (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed, and wherein the integrity block (header) is not transmitted but a

message digest is transmitted.

Clam 22 is rejected as applied above in rejecting claim 18. Furthermore, Bisbee discloses:

The method of claim 18, further comprising the steps of:

sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of:

making a perceivable copy (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed, and wherein the integrity block (header) is not transmitted but a message digest is transmitted;

transmitting the perceivable copy (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed;

receiving the perceivable copy (column 9 lines 50-57, column 10 lines 50-64), wherein the transfer agent (remote location) digitally signs the document;

completing a message digest, creating a digital signature (column 10 lines 23-49), wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature;

transmitting the digital signature (Figure 7, column 10 line 50 – column 11 line 12), wherein the signed document is transmitted to the authentication center (secure environment) for authentication and storage (column 10 lines 4-7);

validating the digital signature (column 10 line 65 – column 11 line 12); and,

generating a revised authoritative record (column 10 line 65 – column 11 line 23), wherein after the signature is validated, the document is confirmed and guaranteed and stored (column 10 lines 1-7), and furthermore, a certificate with all the signature of the Certification Authorities of the signers is appended to the end of the document.

Bisbee does not explicitly disclose generating, at the secure location and transmitting, to a remote location, the partial message digest of the beginning information at the secure environment. Vanstone discloses generating a hash (message digest) of a part (partial) of a document and sending the partial digest to a recipient who can sign the document (column 3 line 65 – column 4 line 26). Bisbee and Vanstone are analogous arts because both are concerned with digitally signing documents, and both use a private key and a digest to calculate the signature. Vanstone states that the "it is usual for the message to include some redundancy" (column 1 lines 47-54) and further states that the accuracy of the message is insured by the hash (digest) (column 2 lines 45-55). Therefore, it would have been obvious to generate the message digest at the secure environment and then transmitting it to the remote location to verify the integrity of the message and provide redundancy in the message.

Claim 23 is rejected as applied above in rejecting claim 19. Furthermore, Bisbee discloses:

The method of claim 19, further comprising the steps of:

sending copies of the revised authoritative record to one or more remote locations by treating the revised authoritative record as the authoritative record and repeating the steps of:

making a perceivable copy (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed, and wherein the integrity block (header) is not transmitted but a message digest is transmitted;

transmitting the perceivable copy (column 9 lines 27-41), wherein a request copy of the document is sent to a transfer agent (remote location) to be signed;

receiving the perceivable copy (column 9 lines 50-57, column 10 lines 50-64), wherein the transfer agent (remote location) digitally signs the document;

completing a message digest, creating a digital signature (column 10 lines 23-49), wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature;

transmitting the digital signature (Figure 7, column 10 line 50 – column 11 line 12), wherein the signed document is transmitted to the authentication center (secure environment) for authentication and storage (column 10 lines 4-7);

validating the digital signature (column 10 line 65 – column 11 line 12);

generating a revised authoritative record (column 10 line 65 – column 11 line 23), wherein after the signature is validated, the document is confirmed and guaranteed and

stored (column 10 lines 1-7), and furthermore, a certificate with all the signature of the Certification Authorities of the signers is appended to the end of the document;

prepending a signature receipt (column 10 line 65 – column 11 line 23), wherein after the signature is validated, the document is confirmed and guaranteed and stored (column 10 lines 1-7), and furthermore, a certificate with all the signature of the Certification Authorities of the signers is appended to the end of the document; and,

appending identifying information (Figure 9, column 10 lines 50-65), wherein a certificate containing the signatures is added to the electronic document.

Claim 24 is rejected as applied above in rejecting claim 18. Furthermore, Bisbee discloses:

The method of claim 18, wherein the step of receiving an electronic record further comprises:

time-stamping the electronic record with a time-stamp that includes a time and date of receipt, and identification information and the time-stamped record is used as the electronic record in the subsequent steps (column 5 line 64 – column 6 line 13).

Claim 25 is rejected as applied above in rejecting claim 18. Furthermore, Bisbee discloses:

The method of claim 18, wherein the first information comprises a digital signature made with a private key of the secure environment (column 5 line 64 – column 6 line 13).

Claim 26 is rejected as applied above in rejecting claim 18 Furthermore, Bisbee discloses:

The method of claim 18, wherein the provable representation of the first information comprises a message digest that was used to generate the first information (column 3 lines 13-20), wherein the second information is interpreted as the message digest and/or signature.

Claim 27 is rejected as applied above in rejecting claim 18. Furthermore, Bisbee discloses:

The method of claim 18, wherein the step of transmitting the perceivable copy, further comprises:

transmitting a cryptographic version of the copy (column 5 lines 28-39, column 6 lines 43-46).

Claim 28 is rejected as applied above in rejecting claim 18. Furthermore, Bisbee discloses:

The method of claim 18, wherein the partial message digest includes information necessary to continue the creation of the message digest at the remote location (column 10 lines 23-49), wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature.

Claim 29 is rejected as applied above in rejecting claim 18. Furthermore, Bisbee discloses:

The method of claim 18, wherein the step of validating further comprises the steps of:

decrypting the digital signature with a public key (column 10 line 65 – column 11 line 13); and,

comparing the decrypted digital signature with a representation of the authoritative record stored in the secure environment (column 10 line 65 – column 11 line 13).

Regarding claim 32, Bisbee discloses:

A method for digitally signing an electronic record received from a secure environment, wherein the electronic record consists of a first portion and a second portion, the method comprising the steps of:

receiving the first portion of the electronic record from the secure environment, wherein the first portion allows a user to view, print or store the electronic record (column 9 lines 50-57, column 10 lines 50-64), wherein the transfer agent (remote location) digitally signs the document;

generating a message digest of the electronic record using the first portion and the partial message digest completing a message digest of the authoritative record at the remote location with the use of the partial message digest and the perceivable copy

(column 10 lines 23-49), wherein the partial message digest is decrypted and then retrieves the encrypted key from the hash (partial message digest) of the document, and is used in conjunction with the digest to produce a digital signature; and,

creating a digital signature of the electronic record using the message digest and a private key (column 10 lines 33-43), wherein the digest is encrypted using the remote location's secret (private) key and produces the signature.

Bisbee does not explicitly disclose generating, at the secure location and transmitting, to a remote location, the partial message digest of the beginning information at the secure environment. Vanstone discloses generating a hash (message digest) of a part (partial) of a document and sending the partial digest to a recipient who can sign the document (column 3 line 65 – column 4 line 26). Bisbee and Vanstone are analogous arts because both are concerned with digitally signing documents, and both use a private key and a digest to calculate the signature. Vanstone states that the "it is usual for the message to include some redundancy" (column 1 lines 47-54) and further states that the accuracy of the message is insured by the hash (digest) (column 2 lines 45-55). Therefore, it would have been obvious to generate the message digest at the secure environment and then transmitting it to the remote location to verify the integrity of the message and provide redundancy in the message.

Regarding claim 33, Bisbee discloses:

The method of claim 32, further comprising the step of:

transmitting the digital signature to the secure environment (Figure 7, column 10 line 50 – column 11 line 12), wherein the signed document is transmitted to the authentication center (secure environment) for authentication and storage (column 10 lines 4-7).

4. Claims 38-42 are system claims analogous to the method claims of 5-10, and therefore, are rejected following the same reasoning.

5. Claims 43-48 are system claims analogous to the method claims of 11-17, and therefore, are rejected following the same reasoning.

6. Claims 49-59 are system claims analogous to the method claims of claims 18-29, and therefore, are rejected following the same reasoning.

7. Claims 60-61 are apparatus claims analogous to the method claims of 32-33, and therefore, are rejected following the same reasoning.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
AU 2131
9/27/05

KA
09/26/2005